나무위키

야한 동영상/은폐와 탐지

최근 수정 시각: 2026-08-04 10:00:54

분류: 성인물 | 컴퓨터 보안 | 프라이버시

상위 문서: 야한 동영상

목차

1. 개요
2. 서론
3. 은폐
  3.1. Tails 사용하기
  3.2. 소프트웨어
    3.2.1. 파일 암호화
    3.2.2. 가상 머신
  3.3. 하드웨어
    3.3.1. 전용 디스크
      3.3.1.1. NAS
        3.3.1.1.1. 라즈베리 파이
  3.4. 인터넷
    3.4.1. 스트리밍
    3.4.2. 클라우드
    3.4.3. 개인용 블로그
  3.5. 기타
4. 탐지
  4.1. 파일 검색
  4.2. PC 기록 추적
  4.3. 급습
5. 결론
6. 번외
  6.1. 소프트웨어
    6.1.1. 헤더 암호화
    6.1.2. 하드디스크 제어
    6.1.3. 파일헤더 조작
    6.1.4. 폴더 미로
    6.1.5. 휴지통
    6.1.6. 파일 합체
    6.1.7. 파일 분산
    6.1.8. 확장자 변경
    6.1.9. 일체화
    6.1.10. 재인코딩
    6.1.11. 파일옵션 조정
    6.1.12. 개인용 계정
    6.1.13. Attrib.exe
    6.1.14. 보안폴더
  6.2. 하드웨어
    6.2.1. 바이오스 암호
    6.2.2. 저장 매체 숨기기
7. 관련 문서

1. 개요

이 문서에 들어온 당신은 **은폐하려는 자**인지, **찾아내려는 자**인지 ~~아니면 **팝콘을 뜯는 자**~~인지를 먼저 파악하고 문서를 읽도록 하자.

인류가 정보화 시대에 돌입한 뒤로 사람들은 컴퓨터에 의존하게 되었으며, 이로 인해 기존에 존재하던 글, 사진, 동영상 등의 정보들은 대부분 하드 디스크를 비롯한 각종 저장소로 옮겨졌다. 거기에 더해 각종 장비들이 소형화되고 휴대가 용이해지며 데이터 유출의 위험 역시 커지고 있다.

여기서 언급되는 기술들은 보안을 요하는 자료를 취급하는 데 있어서도 유효하다. 굳이 야동만이 아니더라도 당신이 국가 최고급 기밀을 다루고 있는 안보 인사거나, 국가 간 협상을 앞두고 있는 장관이나 실무진 또는 군대나 기업의 보안 문서를 보유하고 있는 장교/임원이거나, 중증 환자의 진료 기록을 이용하는 의사나 고객의 개인정보를 가득 정리하고 있는 영업사원이거나, 심혈을 기울여 결말까지 완벽히 만들어낸 소설이나 만화 등을 저장하고 있는 작가 또는 시험 문제를 작성한 교사 혹은 대학 교수 혹은 🔗외장하드를 빌려준 사람, 공인인증서 등의 중요한 데이터를 갖고 있다면 잘 숨겨야 한다는 점에서는 야동하고 다를 바가 없다.

아래에 나열된 방법들은 단순히 주위 사람들의 시선을 피하기 위한 간단한 편법에서부터 전문적인 기술적 암호화까지 다양한 단계를 다루고 있기 때문에 당신이 가장 먼저 고려해야 할 것은 당신의 야동을 **누구로부터** 숨기려는가 하는 것이다. 컴퓨터로 할 줄 아는 거라곤 유튜브, 넷플릭스 재생뿐인 컴맹으로부터 숨길 것인지, 경찰 사이버수사대나 대검찰청, 국가정보원 같은 국가기관의 디지털 포렌식을 상대로 숨길 것인지의 수준을 결정해야 하는 것이다. 타겟이 누구냐에 따라 동원되는 기술의 수준도 달라진다.

이 문서에서는 해당하는 사람들을 위하여 여러 가지 은폐 및 탐지 기술들을 정리했으며 사실 아래 방법들을 적용하더라도, 누군가 당신을 보고 있는 도중 자료를 열람한다면 말짱 도루묵이다. 일을 보기 전에는 반드시 위험요소가 하나라도 있는지 확인하는 것이 바람직할 것이다. 나무위키에서는 이를 위해 별도로 몰컴과 몰컴/은폐와 탐지를 자세히 다루고 있다.

아래에 많은 내용들이 서술되어 있지만, 저 내용들을 실천하기에 앞서서 해야 할 것은 컴퓨터에 암호를 걸어 놓는 것이다. 경찰의 추적을 피하는 게 아닌 이상은 그냥 컴퓨터에 암호만 걸어도 안전한 경우가 많다. 공용컴퓨터라면 데이터를 스마트폰 등에 옮겨서 사용하자.

2. 서론

10대 청소년이 P2P 프로그램(토렌트)으로 다운받을만한 파일의 종류는 정해져 있기 때문에, **가까운 동성 친구**가 아니라면 본인이 야동을 소유한 것을 알아챈 상대가 누구냐에 관계없이 인간관계에 심대한 문제가 생길 소지가 크다. 여기서 '가까운 + 동성 + 친구' 세 단어 중 하나라도 빠지면 안 된다. 만약 한 단어라도 빠졌을 경우를 생각해 보자.

> - **그냥** 친구: 축하한다, 당신은 약점이 잡힘과 동시에 그 사람에게 **변태**로 낙인찍혔다. 특히 동성인 경우는 운이 좋으면 이것을 계기로 '그냥 친구'에서 후술할 '가까운 친구'로 발전하기도 한다. 당신의 성적 지향이 너무 특이한 게 아니면 최소한 사이가 나빠지지는 않는다.
> - 가까운 **이성** 친구: **서로가 서로를 이성으로 보고 있는 경우라면 이보다 더 심각한 참변이 없다.** 특히나 강간, 배빵, BDSM 같이 하드한 요소가 들어갔다면 상대가 이후 손절을 칠 가능성이 높아지며, 특히 당신이 **로리콘**이라면 **귀싸대기 쳐맞는 걸로 끝나는 걸 다행으로 여겨야한다.**[1][2]
> - **친척**: 친한 경우는 그냥 놀리거나 약점이나 잡는 정도이지, 친하지도 않으면 그 시간 이후로 서로 눈도 똑바로 보지 못할 수도 있다.[3]
> - 가까운 **어른**: 가장 편차가 큰 케이스로, 편견이 없는 어른인 경우 사춘기니까 그냥 그러려니 하고 넘길 수도 있지만, **고지식한 어른에게 걸릴 경우엔 최악**으로, 두 번 다시 야동을 못보게 되거나 심지어 이 문서조차도 들어오지 못하게될 수 있다.
> - **가까운 동성 친구**: **공유한다. 여성과 남성을 불문한다.**

물론 가까운 동성 친구라 해도, 당신의 성적 지향에 따라 얼마든지 관계가 틀어질 수 있고, 가까운 이성 친구한테 들켰더라도 별 신경 안 쓰는 경우도 간혹 있다. 그러나 일단 들킨 순간 이루 말할 수 없는 쪽팔림을 느낀다는 사실은 둘째치더라도, 뜻밖의 커밍아웃이 벌어져서 소문이 퍼지는 상황도 있고, 심지어 아동 포르노를 들킨 거라면 얄짤 없이 현행범으로 체포된다.[4]

결론적으로, 앞서 말했듯이 쪽팔림은 당신의 몫이니 가급적 숨기는 편이 좋다는 것을 알 수 있다.

그리고 자취하면 굳이 숨길 필요 없다고도 하는데, **원래 엄마는 갑자기 예고 없이 나타나신다.**

3. 은폐

컴퓨터에 대해 잘 모른다면 아래 방법들을 시도하는 도중 오류가 발생하거나, 심한 경우 컴퓨터에 문제가 발생할 수도 있다. 혹은 기껏 공들였더니 불편하기만 하고 실용성은 없을 가능성도 많다. 각 내용을 직접 해보기 전에 충분한 생각을 거치고 결정하자.

밑의 내용들은 대부분 서로 상충되지 않고 큰 부작용 없이 동시에 사용할 수 있으며, 오히려 최대한 많은 방법들을 동시에 사용하는 것이 권장된다.

3.1. Tails 사용하기

Tails란 아래 번거로운 작업들을 훨씬 편하고 안전하게 사용할 수 있도록 만들어진 리눅스 배포판이다.
Tails OS 문서 참고.

3.2. 소프트웨어

3.2.1. 파일 암호화

방법	암호화 소프트웨어를 이용하여 파일들을 암호화한다.
장점	보안과 편리성, 실용성을 모두 겸비 후술할 대부분의 방법들과 조합할 수 있어 범용성과 활용도 또한 매우 높아 사실상 **자료 은폐의 기본**
단점	검증되지 않은 암호화 프로그램들은 보안상 취약점이 있을 수 있음 비밀번호를 잊어버린다면 파일을 열 수 없음[5] 공용 PC의 경우 주변인에게 의심을 받거나, 열리지 않아 깨진 파일인 줄 알고 삭제해 버리는 경우가 있다.

암호화 소프트웨어는 주로 VeraCrypt[6], BitLocker[7], FileVault[8], 디스크 유틸리티[9]와 같은 프로그램들이 사용된다. 당연하지만, 야동이 아닌 다른 중요한 파일들을 보관하기 위해서 사용할 수 있다.

비밀번호를 모를 경우 사실상 푸는 것이 거의 불가능하기 때문에[10] 매우 안전하고 권장되는 방법이며, 어쩔 수 없이 비밀번호를 말해야 하는 경우가 아닌 한[11] 심지어 VeraCrypt에서는 이런 때를 대비한 특수한 기능을 지원한다. 걱정할 필요가 없을 정도이다. 이것을 악용하여 만들어진 것이 바로 랜섬웨어다.

가능하다면 시스템과 데이터가 저장된 파티션 전체[12]를 암호화하는 것이 좋다. 섬네일이나 임시 파일, 시청 내역 등의 정보가 시스템에 기록되기 때문에 데이터만 암호화한다면 기껏 해놓은 보람도 없이 탈탈 털릴 수 있다.

혹은 탐지자가 컴맹일 경우, 확장자를 바꿀 수도 있다. 예를 들어 보기에서 '파일 확장명'에 체크한 후, 확장자를 txt 같은 걸로 바꾸고 다시 그걸 끄면, 컴맹들은 이걸 보고서도 그냥 깨진 문서 파일이라고 생각할 것이다. 다만 깨졌다고 확인되면 삭제하는 경우도 있으니 주의하자. 물론 용량이 매우 크다는 것을 보고 의심은 하겠지만 물증은 없으니 적당한

핑계거리를 준비해 두자. 단점은 확장자를 mp4로 되돌리는 즉시 회복된다는 것이다.

3.2.2. 가상 머신

방법	가상 머신을 만들고, 그 안에서 중요 파일들을 관리한다.
장점	메인 시스템에는 흔적이 남지 않으므로 기밀성이 유지됨
단점	진입장벽이 높음 메인 시스템 사양이 어느 정도 이상이어야 하므로 비용이 많이 발생함 가상 하드 디스크 파일이 생성되어 이를 안다면 뚫릴 수 있다

일반적으로 VirtualBox, VMware 등의 프로그램이 사용되며, 윈도우 10 Pro 이상의 경우는 윈도우 기본 기능으로 Hyper-V 기능이 있다.[13] 단독으로 사용할 경우 매우 위험이 높으나, 위의 파일 암호화와 함께 사용하여 가상 머신 내부만 암호화할 경우 더욱 안전하고 편리하다. 이는 호스트의 시스템을 암호화하기 곤란한 상황일 때 빛을 발한다. 또한 다중 바탕화면 기능도 유용하니 참고하자. 또한 데이터만 가상머신 디스크 이미지 안에 보관하는 것이 아니라 아예 해당 파일의 다운로드에서부터 엑세스까지 가상머신 내에서만 한다면 메인 시스템 안에는 로그나 섬네일 같은 파일 사용 이력에 관련된 부가 정보들이 남을 가능성도 거의 없어진다.

컴퓨터 사양이 낮다면 게스트 OS로 윈도우보다는 리눅스를 사용하는 게 좋다. 파티션이 ext4 형식이므로 윈도우에서는 읽을 수 없고 대체로 윈도우보다는 가볍다. 물론 약간의 진입 장벽이 추가되지만 윈도우를 불법 복제로 사용하지 않아도 된다. 특히 Raspberry Pi OS Desktop버전을 게스트 OS로 쓰면 어지간한 똥컴에서도 돌아가지만, 야동 시청이 목적이라면 사양이 평균 이상은 되어야 쾌적하다.

가상 머신을 이용할 경우는 가상 하드 디스크 파일이 생성된다는 점에 유의해야 한다. 만일 가상 하드 디스크 파일을 복사해서 마운트를 해버리는 경우가 걱정된다면 vmWare ESXi나 vSphere등의 서버용 가상화 솔루션을 이용해 가상 하드디스크 파일등을 원격지 서버에 두면 된다. 원격지라고 해서 멀리갈것없고 다용도실에 서버를 숨겨두는정도. 이렇게 세팅하고 원격접속한다면 웬만한 컴잘알이어도 서버의 존재를 모른다면 절대 들킬일이 없다. 하지만, 원격지 서버를 이용하는 방법으로 연결 흔적을 지우면서 사용할 바에는 불편하게 한번 더 가상머신을 거치면서 써야 할까라는 의문이 있을 수 있다.

3.3. 하드웨어

하드웨어를 이용할 경우, 돈이 드는 만큼 그 값을 해낸다. 위의 방식들과 합해서 사용할 경우 더욱 강력한 보안을 자랑하거나, 훨씬 편리하고 많은 기능을 사용할 수 있을 것이다.

전용 디스크를 예로 들 경우, 급하면 해당 하드디스크를 뽑아서 비밀장소에 숨기거나, 아예 디가우저로 부수고 파편을 찾아내지 못하도록 흩뿌리면 증거고 뭐고 남지 않기 때문. 최소 수천만 원이나 하는 디가우저는 개인 아닌 하드웨어 전문 파괴업체에서 보유하고 있으므로 그들에게 부숴달라고 하면 된다. 숨길 만한 장소가 없다면 제로필을 해주고 망치나 드릴 등으로 파괴할 수도 있으니...

그리고 SSD는 특성상 파일 복구가 어려워서 제로필을 해줘도 위험의 여지가 남아있는 HDD보다는 안전한 편이다. 물론 그만큼 파일이 날아간다면 복구도 어렵다는 소리가 되므로 양날의 검.[14]

3.3.1. 전용 디스크

방법	전용 외장 HDD나 외장 SSD 또는 USB 메모리를 이용한다.
장점	야동과 일반 파일들을 물리적으로 분리하여 저장할 수 있어 안전함 보관 및 이동이 편리
	OTG 기능을 지원할 경우 스마트폰에서도 사용 가능[15]
단점	용량에 비례해 돈이 상당히 깨진다. 대체로 충격에 약하며 함부로 다루면 고장이 쉽게 발생함 외장 USB의 경우 크기가 작아 잃어버리기 쉬움

하드디스크를 물리적으로 암호화하는 제품도 있다.
이 방법을 사용하는 경우 주의점이 하나 있는데, 야동이 들어 있는지 깜박하고 USB나 외장하드를 다른 사람에게 넘겨주는 일이 발생하는 경우가 있다. 이는 별도의 장소에 외장하드를 보관하거나, 용도에 따라 제조사를 다르게 하여 사용하는 것을 추천한다.

USB를 잃어버리거나 빼앗길 염려가 있다면 USB를 암호화하면 된다. VeraCrypt는 파티션 내에 암호화된 가상 디스크 파일을 만드므로 야동 등만 암호화 드라이브에 저장하고 타인과 공유하는 자료는 바깥에 넣어두면 된다.

3.3.1.1. NAS

방법	NAS를 구매한다.
장점	다른 방법과는 차원이 다른 기능 제공
단점	높은 진입장벽 엄청난 비용 발생 인터넷이 차단되어 있으면 사용 불가 보안 관리를 매우 철저하게 해야 함

다른 방법들과는 차원이 다른 기능을 제공한다. 일부 NAS는 토렌트 부가 기능이 있어 24시간 다운로드도 가능하며, DDNS와 포트포워딩을 활용하면 자체적으로 인트라넷을 구축해서 외부에서도 간편하게 관리할 수 있다.

단점은 NAS 가격 + 전기요금 + 정전 대비 서지 프로텍터 3단 콤보로 인한 엄청난 비용이 발생하며, NAS도 하나의 컴퓨터나 다름없기 때문에 보안 업데이트를 꾸준히 하여야 한다. 또한 진입장벽이 높아 NAS 구축/수정 도중에 디스크를 포맷해 버리는 사태가 발생할 수 있다.

<details>
<summary>3.3.1.1.1. 라즈베리 파이</summary>

방법	라즈베리 파이를 NAS처럼 활용한다.
장점	상술한 NAS의 장점을 그대로 이어받으며, 비교적 저렴하고, 크기가 담배갑 정도라 숨기기 쉽다. 개발용으로도 사용 가능하며, 원하는 기능들을 마음껏 넣을 수도 있다.
단점	상술한 NAS의 단점을 그대로 이어받으며, 고장에 민감하다. 배보다 배꼽이 커지는 상황이 생길 수도 있다.

컴퓨터를 잘 한다면 시도해 볼 만하다. 자세한 내용은 NAS 항목 참고.
</details>

3.4. 인터넷

아래 방법들은 소프트웨어, 하드웨어 방식에 비해 안전성이 떨어진다.

공통적인 사항으로는 인터넷에 연결이 되어 있어야 한다는 점과 로딩이 생기거나 일부 제약이 있으나, 깔끔하고 간편하다. HTTPS가 사용된 사이트, 브라우저(크롬 권장)의 시크릿 모드와 믿을 수 있는 VPN을 사용하는 것이 권장된다.

3.4.1. 스트리밍

방법	별도의 파일을 다운로드하지 않고, 인터넷으로 본다.

장점	컴퓨터에 저장하지 않기 때문에 들킬 확률이 매우 적음 드라이브 용량 절약
단점	데이터 제한 환경이나, 느린 인터넷 회선에서는 사용이 어려움 해당 자료가 삭제되거나 사이트 폐쇄/차단된 경우 시청 불가

3.4.2. 클라우드

방법	파일을 다운로드받은 후, 클라우드에 저장하고 원본은 완전히 삭제한다.[16]
장점	제법 많은 기능 제공 NAS보다 진입장벽이 낮음
단점	해킹 위험이 있음 소수를 제외한 대부분의 국내 클라우드에선 성인물 저장이 금지됨 클라우드 서비스가 종료되면 데이터가 사라질 수 있음 용량이 많을 경우 구독 비용이 발생함 인터넷 차단 시 사용 불가능

최근의 클라우드 서비스는 동영상 파일의 경우 서버에서 스트리밍용 버전을 자동으로 재인코딩해서 마치 유튜브를 감상하듯이 웹 재생을 할 수 있도록 하기도 한다. 구글 드라이브는 약간 구형 버전으로 추정되기는 하지만 아예 같은 기업 산하 서비스인 유튜브의 재생 모듈을 그대로 가져다쓴다. 1초에 수십 시간 분량의 고화질 영상을 인코딩해내는 살인적인 강도의 작업량을 감당하는 유튜브의 인프라를 끌어다 쓸 수 있기 때문에 제공 가능한 돈지랄인 셈.

대부분의 경우 NAS와 장/단점을 공유한다. 또한 NAS와는 다르게 클라우드 운영 사이트에서 어느 파일을 올렸는지 확인이 가능하며 특히 아동포르노에 민감하다.[17] 아예 다운받지 말자. 아동 포르노만 아니라면 구글 드라이브나 드롭박스 같은 해외 서비스에서 트러블이 생길 가능성은 거의 없다. 구글 드라이브의 웹 인터페이스가 아닌 File Stream 같은 기능으로 영상 파일에 접근했다면 File Stream 캐쉬 폴더에 야동이 남아있을 가능성이 높아 이런 방식으로의 파일 접근은 좋지 않을 수 있다.

3.4.3. 개인용 블로그

방법	네이버 블로그나 티스토리, 텀블러 등의 블로그에 비밀글로 저장해둔다. 혹은 비공개 계정의 트위터를 개설해서 그곳에 올린다. 트위터 같은 경우에는 mp4만 저장 가능하고, 영상은 최대 2분 20초를 올리는 것이 가능하다.

클라우드와 마찬가지로, 국내 및 해외의 일부 블로그는 성인물 저장을 금지하고 있다. 성인물의 마지막 피난처와도 같았던 텀블러도 현재 더 이상의 음란물 업로드를 금지하고 있다. 이 방법은 별로 좋지 않은데, 만약 부모가 핸드폰을 켰다가 블로그를 보거나 실수로 글을 공개로 올려버리면...

3.5. 기타

인터넷 방송인이라면 개인방송 등을 하다가 기밀자료를 들키는 사례 역시 생기지 않도록 하자. 실제 사례도 있었다. 또한 보안이 중요한 시설, 아니 그냥 회사나 공공장소에서 그런 짓을 할 생각을 하지 말자. 일본 자위대의 🔗 이지스함 기밀이 유출된 것만 봐도...

4. 탐지

먼저, 타인의 컴퓨터를 마음대로 뒤져보는 것은 굉장한 실례이며,[18] 설령 아래 방법들로 성인물을 찾아냈다고 해도 그것을 퍼트리거나, 놀리거나, 훈계하는 등의 행위는 대상에게 큰 상처가 될 수 있다. 아청법 등에 걸리는 경우가 아니라면 성인이 성인물을 보는 것 자체는 법적으로도 도덕적으로도 전혀 문제될 일이 없으며, 후술할 내용들은 어디까지나 흥미로 읽도록 하자.

4.1. 파일 검색

아래 프로그램들은 컴퓨터 관리에도 적합한 프로그램이다.

- 🔗 Everything: 이름처럼 저장장치의 모든 파일을 검색한다. 설치하거나 포터블 버전을 받아서, 검색어[19]를 입력하고 크기순으로 정렬한 뒤 의심가는 파일 몇 개를 확인하면 끝. 눈치도 없어 숨김 파일이고 시스템 파일이고 뭐고 다 찾아내는 데다가 속도도 빠르다.
- 🔗 Space Sniffer: 폴더의 크기를 시각적으로 보여준다. 폴더나 파일 크기로 타겟을 잡을 때 유용하다. 일일이 수작업으로 큰 파일이 든 폴더를 골라내지 않아도 된다.

4.2. PC 기록 추적

최근 본 문서나 동영상[20]을 확인한다. 보통은 기본 설정을 건드리지 않으니, 이미 정리되어 있거나 설정을 바꾸었다면 의심해 봄 직하다.

운영체제에서 자동으로 만들어내는 섬네일을 활용할 수도 있다. 🔗 Thumbnail Database Viewer와 🔗 thumbcacheviewer로 볼 수 있다.

일부 공유기들은 🔗 접속 로그를 기록하기도 한다. 색다른 방법으로, cmd에서 ipconfig/displaydns를 입력한 후, 성인 사이트가 있는지 확인할 수도 있다.

파일 복구 프로그램을 사용하면 지워진 파일들의 목록을 보거나, 복구할 수 있다.

만약 사용자 계정 등에 비밀번호가 걸려있다면 윈도우 PE나 리눅스 라이브 부팅를 이용하거나, 아예 하드디스크를 뽑아서 직접 확인해 볼 수도 있다.

의외로 백업의 보안은 소홀히 하는 경우도 있다. 굴러다니는 외장 하드디스크나 USB를 살펴보자.

만에하나 공권력이 개입한다면 ISP에 저장된 기록을 살펴볼 수도 있다. VPN을 사용하지 않는다면 여지없이 다 까발려진다.

4.3. 급습

방에 불시에 쳐들어간다. 방문을 마주보게 책상을 배치하거나 모니터에 화장거울로 위장한 백미러를 달면 대비할 수 있다. 또는 문에 센서를 달아서 문열림 감지시 자동 Alt+Tab이 되게 만들 수도 있다. **가능해??**[21]

5. 결론

최종적으로, Tails를 사용하거나, 파일 암호화 + 전용 디스크 + 시크릿 모드 & VPN을 조합해 사용하는 것이 최상의 안전을 확보할 수 있는 길이다. 나머지는 자신의 상황을 고려하여 추가하자.

그러나 대부분의 사람들은 저 정도의 보안이 필요하지 않다. 현실적으로 저 모든 일을 하려면 불편하기 짝이 없으며, 평소에 시크릿 모드를 애용하고, 야동을 숨김으로 설정해놓기만 해도 웬만한 위험은 대비할 수 있다.[22]

설령 들키더라도, 한국은 의외로 성에 개방적인 나라라서 큰 문제가 없고,[23] 잠시 약간의 쪽팔림이 있을 뿐 그냥 생

리적인 현상일 뿐이라 여기며 서로 웃고 넘어가는 경우가 많다. 애초에 성인물을 보는 것(성욕)은 억제가 가능할 뿐, 생물학적으로 당연한 현상이지 전혀 나쁜 일이 아니므로 문제가 될 이유 자체가 없다.[24] 주변에 자신의 약점을 잡으려고 안달이 나있는 사람이 없다면 실수로 다른 사람에게 보이는 경우만 없도록 하자.

물론 성문화를 다 떠나서 상대에게 야동 본다고 놀리거나 훈계하거나 소문을 퍼뜨리는 행위 자체가 남에게 큰 트라우마와 상처를 주는 일이니만큼 상식이 있는 사람이라면 그냥 굳이 찾으려 하지 말고 알더라도 모른 척 해야 한다.

6. 번외

실용성은 없으나, 흥미를 유발할 수 있는 방법들을 정리해두었다.

6.1. 소프트웨어

6.1.1. 헤더 암호화

프로그래밍에 능숙한 사람의 경우는 이러한 경우에 파일을 좀 더 효과적으로 숨길 수 있는 프로그램을 짤 수 있다. 이미 이 단계까지 오면 "숨긴다" 와는 조금 다르지만. 보통 이미지나 동영상 파일, 텍스트 파일이 아닌 이상은 대부분 파일 내용을 인식할 때 파일의 제일 앞부분, 즉 파일 헤더(File Header)를 제일 처음 읽어서 파일의 형식을 파악하기 때문에 이 부분을 **암호화** 시켜놓으면 프로그램에서 제대로 인식하지를 못하기 때문에 어떤 파일인지를 알 수 없다. 동영상 파일의 경우는 재생이 되지 않을 것이며 그림 파일의 경우는 당연히 이미지 자체를 프로그램에서 보여주지 못할 것이다.

암호화는 어떤 암호화든 상관없으며 상대방이 알아보기 어렵고 풀기 간단하면 간단할수록 좋다. 이를 만족시키는 적절한 암호화로는 바로 XOR 연산을 이용한 간단한 암호화가 있다. 보고 싶을 때 암호화를 잠시 풀어두고 다 본 후에는 다시 암호화시키도록 하면 좋을 것이다. 파일 헤더의 크기는 대충 잡아서 4096 바이트로 하자. 어차피 헤더 부분만 암호화시키는 것이므로 0.1초도 채 안 걸린다. C코드 기준으로라면 100줄 내외로 완성시킬 수 있을 것이다. 이 방법은 사실 프로그래밍 난이도 중에서도 상당히 초급에 속한다. ~~파이썬은 2~30줄 내로도 작성 가능하다~~.

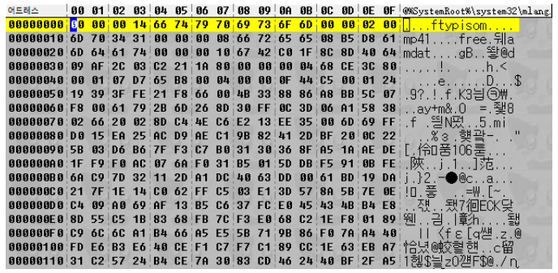
더 간단히 만들자면 magic number만 뭉개버리면 되므로 처음 몇 바이트만 바꿔 줘도 충분하다. 굳이 비밀번호를 만들 필요가 없다면 not연산으로 바꿔 주는 것이 더 간단하다. 그러나 암호화라고 해서 무조건 믿지는 말 것. 이 정도 수준으로 구현 가능한 암호화는 전문인력이 오면 쉽게 뚫린다. 헤더만 섞어놓을 경우 뒷 부분이 온전하므로 더 쉽게 복구가 가능하다. 전문적인 암호화가 필요하다면 차라리 은닉 소프트웨어를 활용하는 것이 낫다.

엄청 간단한 방법 하나를 제시하자면, 야동을 압축하고, 비밀번호를 영문 (대소문자 구별) + 숫자 + 특수문자 이렇게 하면 무차별 대입 공격으로도 천문학적인 시간이 걸린다.

6.1.2. 하드디스크 제어

하드디스크의 랜덤 섹터에 데이터를 기록해 놓은 다음 그 섹터 번호를 기록하여 암호화하는 방식으로 야동을 숨긴다. 이 방법은 파일 자체가 쪼개져 있으므로 숨김 파일 보기 또는 파일 복구 등으로 복구가 불가능하다. 단점으로 해당 하드디스크에 새로운 자료를 기록할 때 야동이 깨질 수 있다는 것과, 파일을 읽는 데 오래 걸린다는 단점이 있다. 이런 단점은 별도의 물리 드라이브를 사용하는 것과 미리 RAM에 파일을 가져오는 것으로 해결 가능하다.

6.1.3. 파일헤더 조작



다음은 mp4 동영상 파일을 hex 에디터로 연 사진이다. 모든 파일에는 확장자 말고도 파일을 구분하기 위해 파일 헤더와 매직 바이트라는 것이 있는데 이 파일 헤더를 바꾸면 다른 파일로 인식하고 열리지 않는다.

예를 들어 위 파일의 파일 헤더의 0x00부터 2바이트를 42 4D (BM)으로 바꾸면 비트맵 파일로 인식하고 동영상 플레이어에서 인식을 하지 않는다.

6.1.4. 폴더 미로

방법	폴더로 미로를 만들어 야동 파일을 깊숙히 숨겨둔다.
장점	작정하고 찾으려 들지 않는 이상 대부분 포기하고 돌아선다.
단점	파일 검색 기능을 이용하면 금방 들통난다. 도리어 내가 미로에 빠질 수도 있다. 폴더를 잠금 해제해서 사용 중일때 비밀번호가 노출된다

가장 간단한 방식으로, 사람들이 게으른 것을 역이용한 방법이다. 정말 게으른 사람들은 이를 하나하나 다 찾지 않는다. 하지만 일단 사람이 미로를 보면 호기심이 샘솟기 마련이다. 어차피 검색하면 다 나온다. 그리고 폴더 속성에서 폴더 안 용량을 볼 수 있어 미로를 해체해 나가며 뚫을 경우 들키는 것은 시간문제다.[25] 게다가 비스타부터 파일 색인이 생기면서 더 빠르고 더 쉽게 찾을 수도 있으며 ZIP 같은 파일도 뚫는다! Windows 10은 더해서, 검색할 필요 없이 시작 → 설정 → 시스템 → 저장 공간 → 드라이브 선택 → 동영상을 클릭하면 동영상이 어느 경로에 있는지 다 나온다.[26] 물론 RAR 같은 다른 압축포맷은 못 찾겠지만, 뭔가 수상한 압축파일이 있다면 풀어서 볼 수도 있다. 정말 불행한 건 **바이러스를 검사하다가도 걸린다.** 폴더명과 경로, 파일 이름까지 하나하나 친절하게 보여주는 데다가 양이 방대하면 방대할수록 미로 폴더의 노출이 길어진다. 귀찮아서 파일명을 안 바꾸면 바로 탄로난다. 그러니 귀찮더라도 파일명은 꼭 바꿔 주자.

진화형으로는 미로형이 아니라 여러 가지 중요한 파일, 숨김 파일들이 수두룩하게 널려 있는 **System32 폴더나 Program files 폴더**의 어딘가에 숨겨놓는 방법이 있다.[27] 특히 이런 폴더 내용물은 손상될 경우 자칫하면 윈도우의 작동이 멈추기 때문에 윈도우 XP의 경우 알아서 컴퓨터 폴더 익스플로러에서 숨긴다. 다만 윈도 내장 검색 기능이 아닌 넥서스파일, 토탈커맨드 같은 전문 관리 프로그램이나 파일의 용량과 특성을 직접 분석하는 프로그램을 쓰면 소용없다. 그리고 이건 역으로 말해서 **파일에 바이러스가 있어도 숨겨줘서 운영체제 개박살 낼 수 있다는** 위험을 내포한다는 것이다. 되도록이면 사용하지 말고, 정 해야 되겠다면 바이러스 검사를 철저하게 한 다음에 하자. 이런 폴더는 워낙 복잡하고 방대하기 때문에 본인도 숨긴 곳을 까먹어 헤매기 쉽다.

좀 더 변형적인 방법으로는 모든 폴더들을 전부 다 시스템 종료 바로가기로 만든 다음에 특정 폴더만 진짜 폴더로 만드는 방법이 있다. 이럴 경우에는 한번 틀리면 컴퓨터가 꺼지므로 인내심이 강한 사람이라도 쉽게 포기하기 마련이다. ~~그래도 뚫을 사람은 뚫는다 하지만 꺼진 후 다시 키려는데 비번이 걸려있다면 어떨까?~~

혹은, 대충 게임 시스템 폴더 안에 (음악 폴더라든가 세이브 파일 같은 폴더는 건드리는 사람도 있으니 적절치 않고 도대체 무슨 용도의 파일인지 모를 폴더가 좋다.)에 미로 폴더를 숨겨두면 그냥 보통 게임 폴더같이 보이게 된다! 이 경우 애당초에 게임파일이기 때문에 용량이 많아도 적절히 넘길 수 있다. ~~그러나 요새는 파일검색 *avi 또는 *.mp4 등으로 이런 꼼수를 무참히 해체해 버리고 있다 그럴 때는 확장자를 변경하면 된다~~.

6.1.5. 휴지통

숨김 옵션이고 뭐고 다 필요 없고 기본 드라이브의 Recycler (윈도우 7 이상에서는 $Recycle.bin)폴더를 이용한다. **물론 윈도우에서**. 안드로이드 같은 곳에 연결 시 망한다. 이 폴더는 정상적으로 표시되지 않으므로 주소 표시줄에 직접 C:$Recycle.bin이라고 적을 필요가 있다.

원래 해당 폴더는 휴지통 폴더인데, 시스템 폴더랍시고 검색에도 안 걸리고 숨김 폴더 표시 처리를 해도 안 나온다. 물론 본격적인 탐색기 프로그램에는 다 뜬다. 휴지통 폴더라고 해서 바탕화면 휴지통 비우면 사라지는 것도 아니다. 그저 숨겨져 있을 뿐. 최근 문서는 사용 후 지우는 것이 기본. 상대방이 recycler의 존재를 알거나 최근 문서로 들키지 않는 한 절대로 들키지 않는다. 어지간하면 여기까지만 해도 안전하다.

6.1.6. 파일 합체

이미지 파일과 zip 파일을 결합하는 방법을 사용할 수도 있다.[28] 이 방식의 숨겨진 단점은, 본인도 어떤 동영상인지 몰라서 하나하나 재생해 봐야 하는 경우가 생긴다는 것이다. 파일명이나 확장자를 바꾸기 전에 txt 파일 등으로 파일명 대조표 같은 걸 만들어 두는 것도 하나의 방법. 아 물론, 그 대조표 파일도 파일명이나 확장자를 바꾸고 암호화도 해놓아야 한다...

6.1.7. 파일 분산

야동 여러 개를 묶어서 분할 압축이 지원되는 압축 형식으로 압축한 다음에 생성된 분할 압축 파일을 분산 저장해 놓는다. 이러면 분산된 분할 압축 파일을 전부 찾아 보기 전까지는 절대 열어볼 수 없다. 아, 압축 파일을 만들 때 암호화는 필수이며 동영상 이름도 바꿔 놓도록 하자. 미로형과 함께 조합하면 시너지 효과가 엄청나다. 단, 분할 압축 파일 확장자(z01, z02, a01, a02 등)를 알면 뚫릴 수 있다. 이는 별도의 하드 디스크나 스마트폰에 숨기는 방식으로 어느 정도 방어할 수 있다. 단점이라면 다시 볼 때 분할 압축된 파일을 전부 모아야 되고, 분할 압축된 파일 중 하나라도 없으면 그 파일은 쓸모가 없다.

6.1.8. 확장자 변경

주변인이 컴퓨터를 어느 정도 하는 것 같으면 확장자를 바꿔서 동영상이 아닌 것처럼 한 다음 자신이 볼 때는 미디어 플레이어로 수동 재생하는 방법도 있다. 확장자명이 동영상 파일이 아니더라도 헤더가 맞는다면 곰플레이어 등에 해당 파일을 드래그하는 것만으로도 정상적으로 재생이 된다. 혹은 은폐하고 싶은 파일의 확장자를 .iso, .bin 등의 가상시디 확장자명으로 바꾸는 것도 효과적이다. 탐지하려는 자가 게임이나 소프트웨어 등의 지식에 무지하다면, "Half-Life 3.iso, menu.json," 처럼 현실에서는 없는 게임/소프트웨어명으로 수정하면 은폐한 사람이 잊어먹을 일이 없다. 가상시디의 용량과 야동의 용량이 엇비슷하기 때문에 정상적인 가상시디 이미지 파일을 모아놓은 폴더에 같이 숨겨놓으면 다른 가상시디 파일들 사이에서 그리 튀지 않기 때문에 용량이 크다는 이유로 걸릴 이유가 없고, 동영상 확장자명이 아니므로 검색을 켜도 섬네일이 드러나지 않는다. 또한 은폐한 파일이 데몬에서 읽히지 않는다고 의심하더라도 그 이미지 파일이 가짜였다거나 깨졌기 때문이라고 변명할 수 있다. 물론 곰플레이어 드래그&드롭 방식을 아는 사람이라면 하나하나 눌러보는 근성을 발휘할 수 있다는 점이 단점이지만, 티가 안 나는 파일들 사이에서 야동 파일 하나를 찾는 것은 결코 쉬운 일이 아니다. ~~리눅스는 확장자를 바꿔도 헤더로 읽기 때문에 소용이 없다.~~

6.1.9. 일체화

무비 메이커나 소니 베가스, 프리미어 프로, 애프터 이펙트 등의 동영상 편집프로그램으로 정상적인 영상 뒤쪽에 야동을 합치는 것이다.

탐지를 할 때 보통 앞부분만 보고 아니다 싶으면 그만 두는 것이 다반사이기 때문에, 상당히 효과적이다. 2시간 반짜리 영화처럼 애당초 길이가 길어 탐지를 포기하게 하거나, 또는 인강과 같은 학술적인 내용의 영상과 합치는 방법이 있다. 혹시라도 들켜도 "나도 속았다"라고 둘러댈 수 있다. 하지만 다시 인코딩을 하는 것이므로 원본 화질이 훼손될 수 있다.

이 방식의 단점은, 가족 영화와 합쳤다가 나중에 합친 사실을 잊고 가족과 함께 보자고 틀었다가 후반부에 갑자기 야동 장면이 나올 수도 있다. 이 경우는 자신만 아는 표시를 해 놓거나 다른 곳에 저장하는 방법이 있고, 어쩔 수 없이 야동이 나왔으면 연기를 하자. 야동이 합쳐져 있던 걸 원래부터 몰랐고 자신도 당황한 척 연기하면 된다.

아니면 자연 다큐멘터리 같은 매우 건전한 영상에 끼워넣으면 된다.

6.1.10. 재인코딩

몇 가지 방어책을 마련해 두어도 화면 미리 보기 옵션이[29] 설정된 경우에는 컴퓨터를 켜놓으면 동영상의 첫 화면이나 특정 화면이 그대로 아이콘으로 나오기 때문에 조금만 인내심을 가진 사람이 있다면 뚫린다.[30] 그리고 일반적으로 일본 야동은 1기가가 넘으므로 화질이 블루레이급 드라마, 애니가 아닌 이상 용량순으로 정렬하면 야동이 맨 위나 아래 쪽으로 싸그리 모이게 된다. 같은 논리로 같은 드라마, 애니라면 재생시간이 거기서 거기이므로 편집을 동일하게 해 놓지 않는 한 길이 순(재생시간 순)으로 정렬해버리면 끝.

상기의 문제점을 해결하기 위해선 인코딩 프로그램으로 동영상의 용량/길이를 맞추고 섬네일을 새로 집어넣는 방법이 있다. 하지만 동영상의 길이만 따지더라도 동영상의 길이가 모두 똑같으면 사람들이 의심할 수 있다. 드라마나 애니메이션 같은 경우, 한 화마다 재생 시간이 조금이나마(1분 ~ 5분 정도) 차이나는 게 당연하므로... 따라서 매우 번거롭고 까다로운 작업을 해야 하기 때문에 야동 하나하나에 일일이 그 짓거리를 하고 있을 정신으로 차라리 다른 방법을 찾는 게 백 배 낫다. ~~그냥 야동을 포기하고 야애니만 보면... 야동이나 야애니나 걸리는 것과 후폭풍은 같다~~ ~~아니 더클 수도 있다~~

6.1.11. 파일옵션 조정

파일의 숨김 옵션을 켜고 파일과 폴더는 아이콘 바꾸기를 이용해 투명한 아이콘으로 바꾸면 시각적으로 거의 눈에 띄지 않는다. 이왕이면 cmd에서 attrib 명령어로 시스템, 읽기 전용, 보관 속성을 전부 켜고 숨기고, 폴더의 제목은 ㄱ+한자키를 동시에 눌러 나오는 특수문자의 1번인 공백으로 하면 폴더의 이름도 보이지 않으니 일석이조. **하지만 누군가가 아이콘 정렬을 시킨다면 멀쩡하게 오와 열을 맞춘 파일들 사이에 이가 빠진 곳이 보인다.** ~~차라리 보이지 않는 폴더로 미로를 만들어라 어떻게 찾으려고 순서로 암기하면 되지~~

보통 특수문자는 오름차순 기준으로 가장 앞에 오게 되어 있으므로, 이가 빠진 곳을 만들지 않기 위해서는 자동정렬-이름-내림차순의 방법을 이용하면 된다. 다만 이 방법을 사용할 시에는 투명 폴더가 위치한 폴더에서는 폴더가 파일 뒤에 오도록 설정해야 한다. 기본 설정으로는 폴더가 먼저 정렬되고 파일이 정렬되기 때문에 파일이 있다면 중간에 수상한(...) 공백이 생기기 때문.

정 아니면 자동정렬을 해제하고 화면 구석에 숨겨버려도 된다. 다만 이 경우는 누가 자동정렬을 사용하면 상기한 빵꾸 문제가 생길 확률이 농후하니 주의할 것.

다음으로 검색에 노출되지 않게 파일의 이름도 바꾸어야 하며 확장자 검색을 피하기 위해서는 확장자도 제거하는 편이 좋다. (일부 운영 체제에서는 섬네일이 노출되므로 .dat등의 확장자로 바꾸어 압축한 뒤 다시 확장자를 제거해도 된다.)

6.1.12. 개인용 계정

말 그대로 개인용 계정을 만드는 것이다. 우선 자신만의 계정을 만든다. 그다음 cmd에다가 net user 자신만의 계정 이름 /active:yes를 친다. 그리고 컴퓨터를 다시 켜면 자신만의 계정이 나와 있는 것을 볼 수 있다. 그리고 끌 때는 net user 자신만의 계정 이름 /active:no를 친다.[31] 하지만 이 방법은 cmd를 조금만 아는 사람이 와도 그 계정에 들어갈 수 있기 때문에 취약하다.[32] 장점으로는 이 방법안에 폴더 미로 만들기 등 거의 모든 방법들을 적용시킬 수 있다는 장점이 있다.

6.1.13. Attrib.exe

https://www.howtogeek.com/105633/how-to-create-a-password-protected-folder-without-any-extra-software/

MS-DOS 시절부터 존재했던 유서 깊은 파일 속성 설정 프로그램.

이 팁은 윈도우가 '보호된 운영 체제 파일 숨기기'와 '숨김파일 표시 안 함'을 기본 설정으로 하고 있는 것을 이용한 배치파일을 설명하고 있다. 파일의 특성을 변경하는 도스 명령어인 attrib.exe를 이용한다.

이 배치파일의 작동 원리는 이렇다.

- Private 나 HTG Locker 라는 폴더 둘 다 없다 → Private 폴더를 만든다.
- Private 폴더가 있다 → Private 폴더를 HTG Locker 라고 이름을 바꾸고, 이 폴더에 시스템 파일 특성, 숨김 파일 특성을 부여한다.
- HTG Locker 폴더가 있다 → 암호를 물어본다. 틀렸다면 종료, 맞았다면 HTG Locker를 Private라고 이름을 바꾸고, 부여했던 파일 속성을 해제한다.

이 배치파일은 굉장히 기초적인 수법을 이용하고 있는데, 이는 암호화가 아니며 보안 대책이라고 불릴 수 없다. 윈도우 탐색기에서 숨김 옵션을 부여해 숨기는 것과 완벽히 동일한 방식이다. (다만, 윈도우 탐색기에서는 시스템 속성을 부여할 수는 없다.)

암호 입력을 받기는 하지만 이 파일은 폴더 내부의 파일의 속성을 변경하지도 않고 폴더 혹은 파일을 암호화하는 것이 아니다. 암호 입력 과정은 단순히 폴더 속성을 변경하기 전에 입력되어 있는 암호와 동일한지만 확인하는 것뿐이다.

이 파일의 단점은 다음과 같다.

- 배치파일의 내용을 이해할 수 있는 사람이 열어본다면 어떤 방법이 적용되어 있는지는 물론 어떤 암호를 적어놓았는지까지 확인이 가능한 단순한 텍스트 파일일 뿐이다. bat2exe나 bat2com 등을 이용해 실행파일로 컴파일 한다면 암호까지는 털리지 않을 수 있겠다.
- 보이지 않는다는 것은 윈도우 설정이 적용되는 윈도우 탐색기에서의 이야기일 뿐, 탐색기의 설정을 해제하거나 기본 설정이 숨김파일 등을 표시하도록 되어 있는 서드파티 프로그램으로 접근하면 충분히 내용물을 볼 수 있다.
- 윈도우 탐색기에서도 HTC Locker라고 직접 경로명을 입력하면 폴더 내부에 접근할 수 있다.
- 윈도우 검색에서 *.avi, *.mp4 등 특정 확장자명으로 검색하면 폴더 내부 파일이 검색이 된다.
- 파일 수와 용량이 숨겨지지 않는다.

이 파일의 사용법은 이렇다.

> 1. 사이트에서 .bat 파일을 복사해서 만든다.
> 2. 파일의 PASSWORD GOES HERE 부분을 지우고 원하는 비밀번호를 넣는다.
> 3. 그 파일을 연다. "Private" 라는 폴더가 상위 폴더에 만들어질 것이다.
> 4. 그 폴더에 야동을 넣는다.
> 5. 파일을 다시 연다. Y를 누른다.
> 6. Private 폴더가 사라진다!

그리고..... 안전성 테스트

> 1. 검색에 Private 을 친다 (물론 사라진 상태에서)
> 2. 클릭해 본다
> 3. 안 통한다! 경로가 올바르지 않다며 **열리지 않는다.**

마지막으로 다시 열려면

> 1. 파일을 연다.
> 2. 비밀번호를 입력한다.
> 3. Private 폴더가 다시 상위 폴더에 뜬다.

이 방법은 일반적인 유저 수준에서는 적절히 이용할 수 있는 팁이 될 수는 있겠으나, 탐지될 수 있는 가능성이 많다.

휴지통 폴더가 동일한 방식에, 보다 간편하면서도 탐지되기는 어렵다는 점에서 추천할 만하다.

6.1.14. 보안폴더

안드로이드 7.0 이후의 삼성 기기들에 기본 탑재되는 Knox 기반의 보안폴더는 내부에 들어간 앱이나 파일을 이용하기 위해선 사용자가 임의로 설정한 보안 솔루션을 풀어야 한다.[33]
특히 보안폴더 내의 앱은 외부의 동일 앱과 설정값 및 데이터를 공유하지 않으며 보안폴더 내 애플리케이션의 내용은 보안 폴더 밖에서 확인할 수 없는데, 애초에 Knox 전용 파티션이 하드웨어적으로 분리되어 있기 때문이다. ~~들킬 걱정 없는 궁극의 야동머신~~ 또한 보안폴더를 보이는 것조차 싫다면 상태창에서 보안폴더를 아예 안 보이게 숨기거나 아이콘 및 이름을 바꿀 수도 있다. 그래도 주의할 점이 있는데, **일반 OneUI에서 보안폴더로 옮긴 경우에는 디지털 포렌식 하면 다 나온다.** 자세한 정보는 해당 문서로

6.2. 하드웨어

6.2.1. 바이오스 암호

방법	컴퓨터의 바이오스에 암호를 건다.
장점	윈도우 PE도 사용 불가능해서 하드디스크를 따로 빼서 찾지 않는 한 탐색이 불가능하다.
단점	공용 컴퓨터에는 적용이 불가능하다. 그리고 정식 수사기관이 개입하거나 컴퓨터의 이상증세로 인하여 암호를 풀어야 하는 상황이 온다면 바로 들통난다. 또한 컴퓨터로 들어오는 전원을 차단하고 본체 내부에 있는 건전지를 뺐다 끼우면 바이오스가 초기화되면서 비밀번호가 무력화된다. 게다가 하드디스크만 빼서 다른 컴퓨터에서 그대로 읽을 수 있다.

6.2.2. 저장 매체 숨기기

500원짜리 딱풀 속에 USB 메모리가 은폐될 수 있다. 물론 아무도 생각 못할 다른 창조적인 방법도 가능하다. 하드웨어 방식의 장점. 인형의 탈을 쓴 USB로 은닉시킬 수도 있지만, 오히려 눈에 띄어 포착될 수도 있다.🔗#

SD카드나 메모리 스틱 같은 메모리 카드와 카드리더기를 결합하는 방식도 있다. 디지털 카메라를 이용하는 입장에서는 야동이 저장된 메모리카드만 조심해서 관리하면 자연스럽게 은닉할 수 있다. 단 이렇게 작은 물건은 잘 분실되고, 비슷한 물건과 섞이면 구분하기도 힘들어서, 야동 SD카드를 보고서 SD카드로 착각하고 제출하거나[34] 가지고 가서는 안 될 곳에 휴대하는 웃지 못할 실수를 저지를 수 있다. 이 경우 야동 전용 메모리의 겉면에 자신만 알 수 있는 표시를 해 놓는 방법으로 불상사를 예방할 수도 있다. 아니면 처음에 구입할 때부터 야동 전용 메모리는 특정 업체의 제품으로 통일하서 구별하는 방법을 쓸 수도 있다.

다양하게 응용하기 좋은 건 마이크로 SD카드다. 가격도 그리 비싸지 않아서 부담도 적은데 개인이 구할 수 있는 저장매체 중 가장 작은 크기라 정말 어디든지 온갖 곳에 숨길 수 있다. 지우개와 지우개 커버 종이 사이에 끼우거나 키보드 스페이스바 밑에다 숨겨 놓기도 하고 모니터의 안 쓰는 포트 단자 사이에 꼽아놓는다든지 전선 정리한 케이블타이 틈에다 끼워두는 등 참으로 다양하다. 작정하고 숨기면 국가의 공권력이 들이닥쳐도 못 찾을 수도 있다. 예를 들어 혁대 버클 뒤쪽 같은 데 숨길 경우 엑스레이 스캐너를 동원해도 못 찾는다. 이 방법의 가장 큰 단점은 어디 있는지 까먹어서 자기도 못 찾는다는 것. 다람쥐가 동면 준비로 여기저기 숨긴 도토리의 상당수는 다람쥐가 까먹는 바람에 먹히지 않고 그대로 다음 해 봄에 싹이 튼다.

또 다른 방법은 다른 형식으로 포맷하는 것이다. 컴퓨터에 가상머신이나 OS를 2개 설치해놓은 뒤 리눅스 전용 확장자로 포맷하고 야동을 담은 뒤 OS는 윈도우를 사용하여 은폐가 가능하다.

일부 디지털 카메라는 해당 카메라로 찍지 않은 사진은 아예 표시하지 않거나 깨진 파일처럼 보여준다! 고용량 SD카드를 끼워놓고 거기에 한두 개 정도 넣은 뒤 자연스럽게 찍고 다니면 된다. 브이로그를 찍는다면 찍어논 폴더에 자연스럽게 분할해서 넣어주면 된다.

7. 관련 문서

- 몰컴/은폐와 탐지
- 비자금
- 몰폰
- 디지털 포렌식
- 야한 동영상/좋은 은폐 방법

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)

기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.